

## Показатели

**Определение:** Показателем остатка  $a$  по модулю  $m$  является наименьшее такое число  $t$ , что

$$a^t \equiv 1 \pmod{m}.$$

Обычно обозначается  $\text{ord}_m(a)$

### Свойства:

- 1 Покажите, что если  $(a, m) = 1$ , то показатель существует
- 2 Покажите, что если  $(a, m) \neq 1$ , то показателя не существует.
- 3 Пусть  $t$  — показатель  $a$  по модулю  $m$ .
  - (a) Докажите, что если  $a^k \equiv 1 \pmod{m}$ , то  $k : t$ .
  - (b) Докажите, что если  $a^{t_1} \equiv a^{t_2} \pmod{m}$ , то  $t_1 \equiv t_2 \pmod{t}$ .
  - (c) Докажите, что числа  $a^0, a^1, a^2, \dots, a^{t-1}$  попарно различны по модулю  $m$ .
- 4 Докажите, что показатели взаимно обратных чисел совпадают.
- 5 Пусть  $\text{ord}_m(a) = t, \text{ord}_m(b) = d$ .
  - (a) Докажите, что если  $t : h$ , то  $\text{ord}_m(a^h) = \frac{t}{h}$ .
  - (b) Докажите, что  $\text{ord}_m(a^h) = \frac{t}{(t, h)}$ .
  - (c) Докажите, что если  $(t, d) = 1$ , то  $\text{ord}_m(a \cdot b) = t \cdot d$ .

### Задачи:

- 1 Найдите  $\text{ord}_{a^n-1}(a)$ .
- 2 Докажите, что  $\varphi(a^n - 1)$  делится на  $n$  для натуральных  $a$  и  $n$ .
- 3 Рассмотрим все числа вида  $10^i - 10^j$  при  $0 \leq i < j \leq 99$ . Сколько из них делятся на 1001?
- 4 Дано нечётное простое число  $p$ , а также простые числа  $q$  и  $r$ . Известно, что  $q^r + 1 : p$ . Докажите, что: либо  $p - 1 : 2r$ , либо  $q^2 - 1 : p$ .
- 5 Сколько делителей от 1 до 200 имеет число  $2^{239} - 1$ ?
- 6 (a) Докажите, что в разложении на простые сомножители числа  $2^q - 1$ , где  $q$  простое, любое число будет давать остаток 1 по модулю  $q$ .  
(b) Выведите из этого, что простых чисел бесконечно много.

- [7] Пусть  $a > 1, p > 2$  и  $p$  простое. Докажите, что простые нечетные делители  $a^p - 1$  или делят  $a - 1$  или сравнимы с 1 по модулю  $2p$ .
- [8] Докажите, что любой простой делитель числа  $2^{2^k} + 1$  сравним с 1 по модулю  $2^{k+1}$ .
- [9] Даны натуральные числа  $a, n > 1$ . Докажите, что для каждого нечетного простого делителя  $p$  числа  $a^{2^n} + 1$  число  $p - 1$  делится на  $2^{n+1}$ .
- [10] Дано простое число  $p$ . Докажите, что  $2^{2^p} - 4$  делится на  $2^p - 1$ .
- [11] Пусть  $p$  и  $q$  простые,  $q > 5$ . Известно, что  $2^p + 3^p$  делится на  $q$ . Докажите, что  $q > 2p$ .
- [12] Докажите, что при натуральном  $n > 1$  число  $2^n - 1$  не делится на  $n$ .
- [13] Найдите все пары простых чисел  $p$  и  $q$  таких, что  $(5^p - 2^p)(5^q - 2^q) \div pq$ .